Docket No.: 1509-280 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Marco Casassa MONT et al.	:	
Serial No. Not yet assigned	:	Group Art Unit: Not yet assigned
Filed: herewith	:	Examiner: N/A

For: DIGITAL CREDENTIAL EXCHANGE

PRELIMINARY AMENDMENT

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Dear Sir:

Preliminary to examination of the above-referenced application, please amend the application:

IN THE CLAIMS:

Please amend claims 12 to 14 and 18 as follows:

12. (Amended) A computer system according to claim 11, further comprising a verifier for verifying the digital certificate.

13. (Amended) A computer system according to claim 11, wherein the first node includes memory for storing the digital credential associated with the secure connection and a display for presenting to a user the digital credential.

14. (Amended) A computer system according to claim 11, wherein a node further comprises a controller for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow a user to monitor digital credentials associated with a secure connection.

18. (Amended) A computer node according to claim 15, further comprising memory for storing the digital credential associated with the secure connection and a display for presenting to a user the digital credential.

REMARKS

The above-referenced application is amended to delete the multiple dependencies and to correct typographical errors of claims 12 to 14 and 18.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached pages are captioned "Marked-Up Version Showing Changes".

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe
Registration No. 19,641

Date: February 20, 2002
1700 Diagonal Road, Suite 310
Alexandria, Virginia 22314
Telephone: (703) 684-1111
Facsimile: (703) 518-5499
AML:eb

8. A method according to claim 1, wherein the secure connection is a secure sockets layer session.

9. A method according to claim 1, further comprising presenting to a user the digital credential associated with the secure connection.

10. A computer system comprising a first computer node coupled to a second computer node via a communication network, the first node and second node being arranged to allow a secure connection to be established between the first and second nodes, the first node having a processor responsive to the interaction of a user for initiating the transfer of a digital credential over the secure connection established between the first node and second node.

11. A computer system comprising a plurality of computer nodes coupled via a communication network, wherein a first node is arranged to allow a plurality of secure connections to be established between the first node and a plurality of other nodes coupled to the network, the first node being arranged to be responsive to the interaction of a user to initiate the transfer of a digital credential over the plurality of secure connections established between the first node and the respective other nodes.

12. A computer system according to claim 11 [or 12], further comprising a verifier for verifying the digital certificate.

13. A computer system according to [any of claims 11 to 12] claim 11, wherein the first node includes memory for storing the digital credential associated with the secure connection and a display for presenting to a user the digital credential.

14. A computer system according to claim [14, wherein a node] at least one of the nodes further comprises a controller for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow a user to monitor digital credentials associated with a secure connection.

15. A computer node for coupling to a second computer node via a communication network, the computer node being arranged to allow a secure connection to be established with the second computer node, the computer node comprising a processor responsive to the interaction of a user for initiating the transfer of a digital credential over a secure connection established between the first node and second node.

16. A computer node according to claim 15, wherein the processor is arranged to receive a digital credential received over the secure connection.

17. A computer node according to claim 15, further comprising a verifier for verifying a digital credential.

18. A computer node according to [any of claims 15] claim 15 further comprising memory for storing the digital credential associated with the secure connection and a display for presenting to a user the digital credential.

19. A computer node according to claim 18, further comprising a controller for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow a user to monitor digital credentials associated with a secure connection.